IN THE DRAWINGS

The attached sheet of drawings includes changes to Fig. 36. This sheet, which includes Fig. 36, replaces the original sheet including Fig. 36.

Attachment: Replacement Sheet

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 4, 8, and 9-18 are pending in the present application, Claims 1, 4, 8, and 9-18 having been amended. Support for the amendments to Claims 1, 4, 8, and 9-18 is found, for example, in Figs. 4, 6, and 35. Applicants respectfully submit that no new matter is added.

In the outstanding Office Action, the related case statement filed on January 31, 2006 was objected to; the specification was objected to; Claim 16 was objected to; Claims 1, 4-6, 8-13, and 16 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement; Claims 1, 4-6, and 8-18 were rejected under 35 U.S.C. §112, second paragraph, as indefinite for failing to particularly point out and distinctly claim the subject matter regarded as the invention; Claims 1, 4-6, 8, 9, 11, and 14-18 were rejected under 35 U.S.C. §102(b) as anticipated by Delayaye et al. (U.S. Patent No. 4,751,733, hereinafter Delayaye); and Claims 10, 12, and 13 were rejected under 35 U.S.C. §103(a) as unpatentable over Delayaye in view of Matsui et al. (U.S. Patent No. 6,201,869, hereinafter Matsui).

The outstanding Office Action has noted that the related case statement filed on January 31, 2006 fails to comply with the provisions of 37 C.F.R. §§1.97, 1.98 and M.P.E.P. §609. Essentially, the Office Action takes the position that the form 1449 is incomplete. With regard to the form 1449 noted as incomplete in the Official Action, Applicants note that the communication referred to is a related case statement,[1] which requires notifying the Examiner of related cases. Accordingly, no form 1449 is believed to be required. As Applicants have furnished this information to make the Examiner aware of

[1] See MPEP § 2001.06(b).

other applications, and no such format is required of such information, Applicants respectfully submit that no further corrective filings is required.

With respect to the objection to the specification for failing to provide a proper antecedent basis for the claimed subject matter, Applicants respectfully submit that this objection is moot in light of the amendments to the claims.

With respect to the objection to Claim 16, Claim 16 is amended to correct the informality identified in the outstanding Office Action.

With respect to the objection of Claims 1, 4-6, 8-13, and 16 under 35 U.S.C. §112, first paragraph, Applicants respectfully submit that this ground of rejection is moot in light of the amendments to the pending claims.

With respect to the objection of Claims 1, 4-6, and 8-18 under 35 U.S.C. §112, second paragraph, Applicants respectfully submit that this ground of rejection is moot in light of the amendments to the pending claims.

Fig. 36 is amended to add reference numeral 1004. The specification is also amended to describe the item identified by reference numeral 1004. Applicants respectfully submit that no new matter is added.

As described in the present specification, page 48, line 13 to page 49, line 26, the security against SQUARE attack can be improved by adding given conditions to the combination in the higher-level MDS 104 (the combination relationship among input and output bits of the higher-level MDS or the interconnect relationship among operational paths). With reference to annotated Fig. 35 (filed herewith), the given conditions are to double or multiply all or part of differential paths (operational paths between the first-half S-boxes 1001 of the preceding extended S-box 103 and the first-half S-boxes 1002 of the succeeding extended S-box 103) (i.e., to make fan-in two or more). Thus, a high avalanche

effect can be achieved and the number of stages that are subject to SQUARE attack can be reduced by one in comparison with the conventional technique.

An arrangement of the higher-level MDS 104 will be described with reference to Figs. 28 through 35 of the present application. In each figure, it is supposed that data flows from the top side to the bottom side. In this example, the higher-level MDS 104 is arranged such that the fan-in is set to two or more for all of the differential paths.

As described in the present specification, page 50, lines 1-8, Fig. 28 illustrates the MDS portion 104-1, which performs the processing on the leftmost bit of eight bits from each S-box (16-bit data or four sets of 4 bits of data) included in the preceding extended S-boxes 103. Fig. 29 of the present application illustrates the MDS portion 104-8 which performs the processing on the rightmost bit of eight bits from each S-box.

As described in the present specification on page 52, line 10 to page 53, line 16 and shown in Fig. 35, the first-half S-boxes 1001 in the preceding extended S-box 103 and the first-half S-boxes 1002 in the succeeding extended S-box 103 are connected together through the second-half S-boxes in the preceding extended S-box 103. At this point, the higher-level MDS (104-1 to 104-8) is arranged based on the following criterion: any one of the S-boxes (a total of 16 S-boxes in this example) in the first-half of the preceding extended S-box 103 and any one of the S-boxes (a total of 16 S-boxes in this example) in the first-half of the succeeding extended S-box 103 are interconnected (coupled) by two or more paths.

For example, an S-box 1001 in the first-half of the preceding extended S-box and an S-box 1002 in the first-half of the succeeding extended S-box 103 are interconnected by two paths indicated by bold lines as shown in Fig. 35. Other S-boxes are also interconnected by two to four paths.

In contrast, with the conventional SQUARE encryption/Rijndael encryption, an S-box 1003 in the first-half of the preceding extended S-box and an S-box 1004 in the first-half of

the succeeding extended S-box 103 are interconnected by only one path (fan-in = 1) as shown in Fig. 36 and the same is true of other S-boxes. Therefore, the avalanche effect is low.

In a non-limiting embodiment of the claimed invention, encrypting sections are connected in series. Each of the encrypting sections (101) comprises extended S-boxes (103), and a higher-level MDS (104). Each of the extended S-boxes (103) comprises first-half S-boxes (112), a lower-level MDS (113), and second-half S-boxes (112). Any one of the first-half S-boxes (112) is connected to any one of the first-half S-boxes (112) in the succeeding encrypting section via at least two paths.

Turning now to the outstanding rejections based on art, Applicants respectfully submit that the amendment to Claim 1 overcomes the outstanding ground of rejection. Amended Claim 1 recites, *inter alia*, "wherein any one of the first subunits is connected to any one of the first subunits in the succeeding encrypting section via at least two paths."

Delayaye does not disclose or suggest that any one of the first subunits is connected to any one of the first subunits in the succeeding encryption section via at least two paths. Figs. 5 and 6 of Delayaye show the diagram used for performing the permutation operations, in which each bit is connected to only one bit. The outstanding Office Action takes the position that Delayaye discloses that each substitution unit is connected to each succeeding corresponding substitution unit by multiple paths. However, assuming *arguendo*, that the Office Action is correct, the substitution unit of Delayaye does not equate to the claimed "first subunits." As described in amended Claim 1, the "first units" include "first subunits," and it is these "first subunits" that are connected to any one of the first subunits in the succeeding encrypting section via at least two paths.

Matsui does not cure the above-noted deficiency in amended Claim 1. Matsui merely discloses a nonlinear transformer 131 including the Galois Field inverse circuit 152.

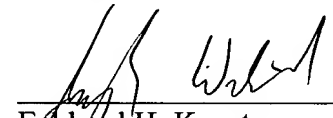
In view of the above-noted distinctions, Applicants respectfully submit that amended Claim 1 patentably distinguish over Delayaye and Matsui, taken alone or in proper combination.

Claims 4, 8, and 12-18 recite elements similar to those of amended Claim 1. Thus, Applicants respectfully submit that Claims 4, 8, and 12-18 (and Claims 9, 10, and 11 dependent thereon) patentably distinguish over Delayaye and Matsui, taken alone or in proper combination, for at least the reasons stated for Claim 1.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Joseph Wrkich
Registration No. 53,796

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JW\210580US\210580US_AM DUE 1-14-06.DOC

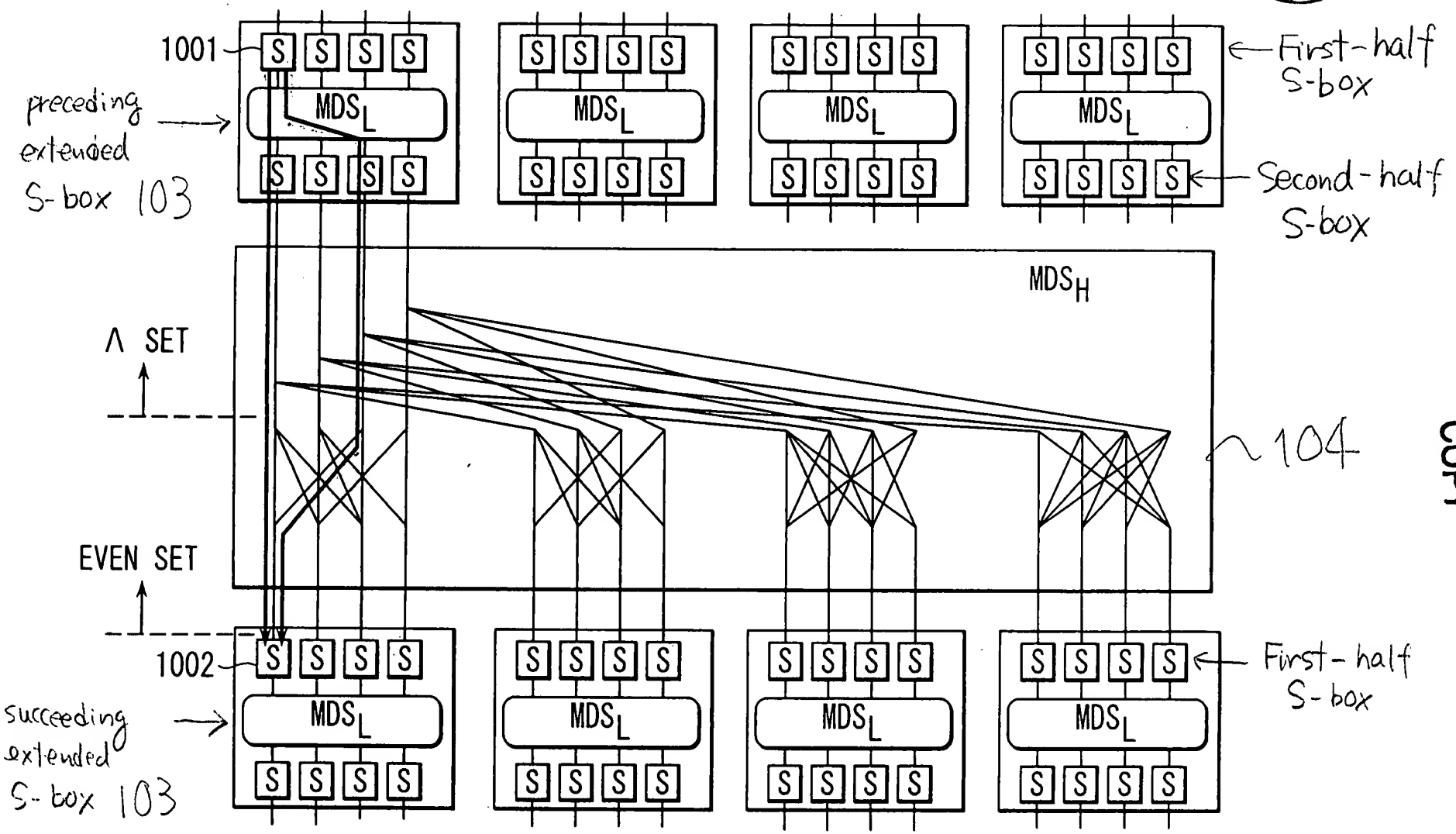


FIG. 35